ZAISTENIE ELEKTRONICKÉHO DÔKAZU VO SVETLE REKODIFIKÁCIE TRESTNÉHO PORIADKU

TOMÁŠ ABELOVSKÝ[*]

ANOTACE

Predmetom tejto krátkej úvahy je zamyslenie sa nad inštitútom elektronického dôkazného prostriedku, jeho úskaliami a súčasnými tendenciami, ktoré by nemali ostať opomenuté v pripravovanom trestnom procesnom kódexe. Zaujímavým a často diskutovaným spôsobom získavania dôkazov je zvláštna ediční povinnosť na uchovávanie a vydanie inkriminovaných počítačových údajov, resp. dát. Táto povinnosť je zakotvená v § 90 TP SR. Môže sa zdať, že tento procesný inštitút môže slúžiť ako vhodná inšpirácia pre súčasné legislatívne práce v ČR. V úvahe bude poukázané aj na jeho nedostatky a možné spôsoby nápravy.

KLÍČOVÁ SLOVA

elektronický dôkazný prostriedok, dátový nosič, dokazovanie, zaistenie dôkazu

ABSTRACT

The subject of this short paper is the reflection on institute of electronic evidence, on its difficulties and present tendencies, which should not be forgotten in the upcoming Code of Criminal Procedure. An interesting and often discussed way of collection of evidence is special obligation to safeguarding and surrendering incriminating computer stored information (resp., data). The obligation is based in the Section 90 of Slovak Code of Criminal Procedure. It may seem that this procedural institute can serve as an appropriate inspiration

[*] Autor je doktorským studentem Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontaktní e-mail: tomas@abelovsky.com

for the current legislative works in Czech Republic. Also, the discussion shall highlight its deficiencies and possible means of redress.

KEYWORDS

electronic evidence, data storage, evidencing, seizing of evidence

1. ÚVODNÉ POZNÁMKY

Elektronický, resp. digitálny dôkazný prostriedok[1] v súčasnom trestnom konaní predstavuje jeden z kľúčových nástrojov získavania dôkazov.[2] V dobe rozmachu kyberkriminality a sofistikovaného organizovaného zločinu sa vyťažovanie počítačových systémov pre účely ďalšieho forenzného skúmania stalo dennou rutinou orgánov činných v trestnom konaní. Tie sú konfrontované s neutíchajúcim technologickým pokrokom a sústavnou rafinovanosťou páchateľov. Avšak na druhej strane tu stojí základné právo na spravodlivý súdny proces vyšetrovanej osoby, ktorá sa v postavení účastníka konania aktívne zaujíma o spôsob, formu a účel zaistenia elektronického dôkazného prostriedku.[3] Napätie medzi týmito dvoma záujmami je riešené predovšetkým procesnou kodifikáciou trestného práva. Tá by mala predstavovať základ pre správne zbieranie (zaisťovanie), vykonávanie a hodnotenie dôkazov. Zmyslom dokazovania je overenie si určitého tvrdenia, čo predstavuje myšlienkový proces zrekonštruovania minulých dejov. Preto, nový fenomén elektronického dôkazného prostriedku posúva paradigma vnímania procesu dokazovania do úplne novej roviny. Pri každom dokazovaní po získaní požadovanej informácie, pristupuje logická operácia podradenia skutkovej (dejovej) podstaty pod zodpovedajúcu právnu normu.[4] Navyše, pre dokazovanie elektronickými dôkaznými prostriedkami bude priliehavosť voľby právnej normy súdom

[1] Anglo-americká právna úprava hovorí o *e-evidence, digital evidence* alebo *electronic stored information.*

[2] Táto skutočnosť je daná aj tým, že podiel elektronických dát v podnikovom sektore sa za posledných 15 rokov zvýšil z 20% na 90%. Viď. Forenzní služby: eDiscovery. In: PWC Česká Republika, s.r.o. [online]. [cit. 2015-06-12]. Dostupné z: http://www.pwc.com/cz/cs/forenzni-sluzby/assets/pwc-vyhledavaci-technologie.pdf

[3] Viď. napr. Rampášek, M. Ústavnoprávne garancie pri uchovaní a vydaní počítačových údajov. Bulletin slovenskej advokácie. ISSN 1335-1079. Roč. 19, č. 6. 2013.

[4] Podľa Knappa môžeme hovoriť, že súčasťou aplikácie práva je práve táto operácia - subsumpcia. Viď. KNAPP, Viktor. Teorie práva. Praha : C.H.Beck, 1995. ISBN 80-7179-028-1. s. 187.

okrem iného závislá aj na tom, ako dobre bude zistená samotná skutková podstata prostredníctvom vykonávania takýchto dôkazov.[5] Je preto dôležité sledovať, ako bude vyzerať úprava zaisťovania elektronických dôkazov v novom procesnom kódexe.

Pripravovaná rekodifikácia trestného poriadku v ČR si kladie za cieľ zrýchliť trestné konanie, posilniť význam štádia konania pred súdom, zvýšiť aktivitu procesných strán a stanoviť procesnú zodpovednosť štátneho zástupcu za nevykonanie dôkazu v potrebnom rozsahu (formálne dôkazné bremeno).[6] Okrem toho, že pred súdom bude zvýraznený princíp kontradiktórnosti, nový trestný poriadok počíta so samostatnou úpravou absolútne neúčinných dôkazov. Ako je vidieť, nový kódex precizuje dokazovanie a stranou neostáva ani súčasný inštitút zaistenia veci. Východiska a princípy nového trestného poriadku počítajú v nadväznosti na rozvoj používania elektronických prostriedkov s novou úpravou zaisťovania dát z počítača a iných elektronických zariadení, a to aj spôsobom na diaľku. Rozhodovacia prax ukázala, že zaisťovanie dát dostáva nový rozmer a vymaňuje sa zo zaužívaného inštitútu zaisťovania veci. Príkladom môže byť nedávne rozhodnutie Ústavného súdu ČR, kde sa okrem povahy sociálnej siete riešil aj spôsob nešťastne predloženého elektronického dôkazu – printscreenu počítačovej obrazovky (sociálnej siete Facebook) policajným vyšetrovateľom.[7] O konkrétnych detailoch rekodifikácie pracovná komisia zatiaľ mlčí, ale pre potreby tejto práce je potrebné predstaviť možnosti komparatívneho pohľadu so slovenskou procesnou úpravou.

2. ZAISTENIE DÁTOVÉHO NOSIČA ALEBO DÁT?

Súčasná právna úprava v prípade využitia zaisťovacieho prostriedku v prípravnom konaní alebo konaní pred súdom počíta so všeobecnou

---

[5] Abelovský, T. Elektronický dôkazný prostriedok vo svetle práva duševného vlastníctva. In: Cofola 2014: the conference proceedings. 1. vyd. Brno: Masaryk University, 2014. Spisy Právnické fakulty Masarykovy univerzity v Brně, sv. 483. ISBN 9788021072114. s. 185.

[6] MS ČR: Komise pro nový trestní řád. Věcný záměr trestního řádu - hlavní principy navrhované rekodifikace trestního práva procesního [online]. [cit. 2015-06-12]. Dostupné z: http://www.ceska-justice.cz/wp-content/uploads/2014/04/hlavn%C3%AD_principy_1.pdf

[7] Rozhodnutie Ústavného súdu ČR zo dňa 30.10.2014 spis.zn. III.ÚS 3844/13. [online]. [cit. 2015-06-12]. Dostupné z: http://www.usoud.cz/aktualne/?tx_ttnews%5Btt_news%5D=2746&cHash=2a4e443657acf7a2db351b9cac9264f8

edičnou povinnosťou zakotvenou v § 78 TŘ ČR.[8] V praxi sa často tento inštitút využíva spolu s domovou prehliadkou podľa § 82 až § 85b TŘ ČR. Navyše, podľa zjednocujúceho stanoviska NSZ, zaistenie aktuálneho stavu emailovej schránky (online služba umožňujúca uloženie dát prijatej, rozpísanej, odoslanej a zmazanej elektronickej komunikácie) je možné vykonávať aj v súlade s inštitútom sledovania osôb a vecí podľa § 158 odst. 1, 3 TŘ ČR.[9] Avšak, platný trestný poriadok nerobí rozdiel v otázkach zaistenia dôkazných prostriedkov medzi vecou a elektronicky uloženou informáciou, resp. dátami. Orgány činné v trestnom konaní sa k dôkazom dostávajú prostredníctvom vyťažovania zaistených elektronických nosičov (vecí) za využitia odbornej znaleckej expertízy. Táto koncepcia je však prekonaná, nakoľko už dávno nie sme svedkami toho, že by páchatelia nechávali svoje elektronické stopy len na USB kľúčoch, pevných diskoch, cédečkách alebo na už historicky znejúcich disketách (hmotných predmetoch). Kyberpriestor v súčasnosti predstavuje nový fenomén, ktorý umožňuje virtualizovanie dát do takej podoby, že tie sú fyzicky nelokalizovateľné.[10] Čo je však dôležitejšie, zaistenie dát na rozdiel od zaistenia veci (napr. celého hard disku počítača) môže priniesť omnoho šetrnejší a precíznejší zásah do práv vyšetrovaného. Ide o vyjadrenie zásady zdržanlivosti a primeranosti, resp. minimalizácie a subsidiarity, ktoré sú vlastné trestnému právu.[11]

---

[8] „Kdo má u sebe věc důležitou pro trestní řízení, je povinen ji na vyzvání předložit soudu, státnímu zástupci nebo policejnímu orgánu; je-li ji nutno pro účely trestního řízení zajistit, je povinen věc na vyzvání těmto orgánům vydat.“ Viď. § 78 odst. 1 zákona č. 141/2014 Sb. o trestním řízení soudním (trestní řád) In: Beck-online [právní informační systém]. Nakladatelství C. H. Beck [online]. [cit. 2015-06-12]. Dostupné z: http://www.beck-online.cz/

[9] „Aktuální obsah e-mailové schránky je určován vůlí uživatele a lze jej zjišťovat postupem podle § 158d odst. 3 trestního řádu, který je možno považovat za zákonnou licenci prolamující ústavně zaručené právo na ochranu soukromí v e-mailové schránce se nacházejících záznamů, a to podle platné právní úpravy v případě trestního řízení pro kterýkoli úmyslný trestný čin.“ Viď. Stanovisko č.1/2015 NSZ ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek [online]. [cit. 2015-06-12]. Dostupné z: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf

[10] Napr. cloud systém, ktorý využíva serverové farmy po celom svete a ani sám správca tohto systému nevie, kde sa nachádza ten ktorý sektor disku s požadovanou informáciou, nakoľko tieto môžu byť v neustálom pohybe.

[11] Kolouch, J. Zajišťovací úkony a důkazní prostředky využitelné v rámci boje s kybernetickou trestnou činností. [online]. [cit. 2014-01-12]. Dostupné z: https://csirt.cesnet.cz/Dokumenty?
action=AttachFile&do=get&target=Zajistovaci+ukony-RTF.pdf

Budapeštiansky dohovor o počítačovej kriminalite (ďalej len ako „Dohovor“)[12] definuje počítačové údaje ako akékoľvek znázornenie faktov, informácií alebo pojmov vo forme, ktorá je vhodná na spracovanie v počítačovom systéme, vrátane programu umožňujúceho nariadiť výkon nejakej funkcie počítačovým systémom. Ďalej o prevádzkových údajoch hovorí, že ide o akékoľvek počítačové dáta, ktoré súvisia s komunikáciou prostredníctvom počítačového systému, sú generované počítačovým systémom, ktorý tvoril súčasť reťazca komunikácie, s uvedením pôvodu, cieľa, trasy, času, dátumu, objemu, trvania komunikácie alebo typu základnej služby. Počítačové údaje môžu byť súčasťou jedného alebo viacerých dátových nosičov. Môžu byť zašifrované a navonok vystupovať ako prázdne nezapísané miesto dátového nosiča. Môžu byť rovnako schované v inom dátovom formáte (napr. steganografia). Navyše nikdy nemusia byť uložené v celku a na jednom fyzickom mieste (napr. packaging). Ich vlastnosťou je potencionálna ubiquita a volatilita. Potencionálna ubiquita predstavuje pojmový znak predmetu, ktorý je v nehmotnej podobe a ktorý sa vyznačuje schopnosťou byť všadeprítomný. Môže byť kedykoľvek a kdekoľvek vnímaný (napr. webstránka s protiprávnym obsahom, pirátska kópia audiovizuálneho diela šírená sieťou P2P). Taktiež ho môže užívať (prezerať) neobmedzený počet ľudí. Čo je zásadné, toto užívanie nemusí ovplyvňovať jeho podstatu a funkciu. Na druhej strane volatilita alebo volatilnosť (z angl. volatility) je v ekonomických vedách pojem užívaný pre kolísavosť, nestálosť, prchavosť, resp. premenlivosť hodnôt. Táto vlastnosť však výstižne popisuje základnú črtu elektronických dát. Totiž každý elektronický alebo digitálny záznam sa môže pomerne jednoducho a nepozorovane (aj automaticky) modifikovať alebo zmeniť. Takáto zmena je spôsobená povahou alebo okolnosťami, za ktorých bolo s týmto záznamom nakladané. Inak povedané, už len samotným kopírovaním záznamu dát sa môže kontaminovať ich obsah. Kľúčom k elektronickému dokazovaniu je práve pochopenie tejto vlastnosti – volatility elektronického dôkazného prostriedku v počiatočnej fáze – zaisťovania počítačových údajov. Aj keď ide o pomerne náročné technické vedomosti o spôsobe zberu, nakladania a uchovávania dát výpočtovej

[12] Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě č.104/2013 Sb. medzinárodných smluv ČR. [online]. [cit. 2015-06-12]. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=26438

techniky, už samotná vedomosť o možnej volatilite napovie o správnej voľbe postupov. Navyše, pre správne technické postupy musí existovať opora v trestnom poriadku.

3. ZAISŤOVANIE POČÍTAČOVÝCH ÚDAJOV VO SVETLE SLOVENSKÉHO TRESTNÉHO PRÁVA

3.1 ZÁKONNÉ USTANOVENIE

Slovenská právna úprava priniesla vo svojej rekodifikácii trestného poriadku (ďalej ako „TP SR“) z roku 2005 v štvrtej hlave o zaistení osôb a vecí v § 90 špeciálnu úpravu uchovania a vydania počítačových údajov:[13]

> § 90 Uchovanie a vydanie počítačových údajov
>
> *(1) Ak je na objasnenie skutočností závažných pre trestné konanie nevyhnutné uchovanie uložených počítačových údajov vrátane prevádzkových údajov, ktoré boli uložené prostredníctvom počítačového systému, môže predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor vydať príkaz, ktorý musí byť odôvodnený aj skutkovými okolnosťami, osobe, v ktorej držbe alebo pod jej kontrolou sa nachádzajú také údaje, alebo poskytovateľovi takých služieb, aby*
>
> a) také údaje uchovali a udržiavali v celistvosti,
>
> b) umožnili vyhotovenie a ponechanie si kópie takých údajov,
>
> c) znemožnili prístup k takým údajom,
>
> d) také údaje odstránili z počítačového systému,
>
> e) také údaje vydali na účely trestného konania.
>
> (2) V príkaze podľa odseku 1 písm. a) alebo písm. c) musí byť ustanovený čas, po ktorý bude uchovávanie údajov vykonávané, tento čas môže byť až na 90 dní, a ak je potrebné ich opätovné uchovanie, musí byť vydaný nový príkaz.
>
> (3) Ak uchovávanie počítačových údajov vrátane prevádzkových údajov na účely trestného konania už nie je potrebné, vydá predseda senátu

[13] Viď. § 90 zákona č. 301/2005 Zb. Trestný poriadok In: Jednotný automatizovaný systém právnych informácií [online]. [cit. 2015-06-12]. Online. Dostupné z: http://jaspi.justice.gov.sk

> a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor bez meškania príkaz na zrušenie uchovávania týchto údajov.
>
> *(4) Príkaz podľa odsekov 1 až 3 sa doručí osobe, v ktorej držbe alebo pod jej kontrolou sa nachádzajú také údaje, alebo poskytovateľovi takých služieb, ktorým sa môže uložiť povinnosť zachovať v tajnosti opatrenia uvedené v príkaze.*
>
> *(5) Osoba, v ktorej držbe alebo pod jej kontrolou sa nachádzajú počítačové údaje, vydá tieto údaje, alebo poskytovateľ služieb vydá informácie týkajúce sa týchto služieb, ktoré sú v jeho držbe alebo pod jeho kontrolou, tomu, kto vydal príkaz podľa odseku 1 alebo osobe uvedenej v príkaze podľa odseku 1.*

Podľa tohto ustanovenia ide o situáciu, kedy na objasnenie skutočností závažných pre trestné konanie je nevyhnutné uchovanie, resp. vydanie uložených počítačových údajov vrátane prevádzkových údajov. Tento zaisťovací úkon nie je podmienený výpočtom špecifických trestných činov. Navyše, použitie § 90 TP SR nie je v aplikačnej praxi jednoznačné a prináša nedorozumenia, kedy sa toto ustanovenie má využiť.[14] V nasledujúcej časti budú rozobraté jednotlivé podmienky použitia tohto ustanovenia.

3.2 POČÍTAČOVÉ A PREVÁDZKOVÉ ÚDAJE, OTÁZKA ICH VZNIKU

Tak ako Dohovor, aj zákon rozlišuje dve samostatné kategórie údajov. Zákon priamo neuvádza, či v čase vydania príkazu už musia údaje existovať a musia byť uložené prostredníctvom počítačového systému. Dôvodová správa k zákonu sa obmedzuje na konštatovanie že, „[ú]prava reaguje na dohovor Rady Európy o počítačovej kriminalite, ktorý bol prijatý členskými štátmi Rady Európy dňa 23.11.2001 v Budapešti. Toto ustanovenie umožňuje vydať príkaz na uchovanie a vydanie počítačových dát pre účely trestného konania, najviac na 90 dní. Príkaz na uchovanie a vydanie počítačových dát, ak sú potrebné na účely trestného konania je možné vydať opätovne.“[15] Súčasná odborná literatúra je veľmi skromná

[14] Rampášek, M. Uchovanie a vydanie počítačových údajov v trestnom konaní. Bulletin slovenskej advokácie. ISSN 1335-1079. Roč. 19, č. 5 (2013), - s. 21-26. Lit.

[15] MS SR. Dôvodová správa, Všeobecná časť, Podľa Plánu legislatívnych úloh vlády SR na rok 2003 sa predkladá do legislatívneho procesu návrh nového Trestného poriadku. Epi.sk. Elektronické právne informácie. [online]. [cit. 2015-06-12]. Dostupné z: http://www.epi.sk/dovodova-sprava/Dovodova-sprava-k-zakonu-c-301-2005-Z-z.aspx

a obmedzuje sa na konštatovanie, že „účelom tohto inštitútu je najmä odhaľovanie a vyšetrovanie trestnej činnosti páchanej prostredníctvom internetu.“[16] V praxi sa objavuje názor, že by mohlo ísť aj o údaje prenášané v reálnom čase (najmä z dôvodu možného zaistenia reálne prenášaných prevádzkových údajov). S týmto názorom sa však nie je možné stotožniť. Účel tohto ustanovenia smeruje iba k uchovaniu už prenesených (uložených) údajov (a to vrátane uložených prevádzkových údajov). Teda ide o zaistenie počítačových údajov už zapísaných na pevnom nosiči. Taktiež, gramatickým výkladom je možné dospieť k tomu, že ide o minulé údaje (t.j. tie, ktoré boli uložené prostredníctvom počítačového systému). Navyše, Dohovor rozlišuje medzi urýchleným uchovaním uloženým počítačových údajov (článok 16), urýchleným uchovaním a čiastočným sprístupnením prevádzkových údajov (článok 17), zhromažďovaním údajov v reálnom čase (článok 20) a zachytením obsahových údajov (článok 21). Predmetné zákonné ustanovenie však kopíruje povinnosti uvedené v ustanoveniach o urýchlenom uchovaní uložených počítačových údajov (článok 16)[17] a prehliadke o zaistení uložených počítačových údajov (článok 19).[18]

3.3 OPRÁVNENÝ ORGÁN A POVINNÁ OSOBA

Právomoc na vydanie tohto príkazu má pred začatím trestného stíhania alebo v prípravnom konaní prokurátor, v ostatných prípadoch predseda senátu.

Príkaz môže smerovať voči osobe, v ktorej držbe alebo pod ktorej kontrolou sa nachádzajú počítačové údaje alebo voči poskytovateľovi

[16] Minárik, Š. Trestný poriadok. Stručný komentár. 2010. Iura edtion s.r.o. str. 315 an.

[17] Čl.16 ods. 1 Dohovoru: „Každá strana prijme potrebné legislatívne a iné opatrenia, aby umožnila jej príslušným orgánom nariadiť alebo podobným spôsobom zabezpečiť urýchlené uchovanie určených počítačových údajov vrátane prevádzkových údajov, ktoré boli uložené prostredníctvom počítačového systému, najmä ak existujú dôvody domnievať sa, že hrozí osobitné riziko straty alebo pozmenenia týchto počítačových údajov.“

[18] Čl.19. ods. 3 Dohovoru: „Každá strana prijme potrebné legislatívne alebo iné opatrenia na udelenie oprávnenia jej príslušným orgánom zaistiť alebo podobne zabezpečiť počítačové údaje, ku ktorým získali prístup podľa odseku 1 alebo 2. Tieto opatrenia zahŕňajú oprávnenie zaistiť alebo podobne zabezpečiť počítačový systém alebo jeho časť, alebo pamäťový nosič počítačových údajov, vyhotoviť a ponechať si kópiu týchto počítačových údajov, zachovať celistvosť relevantných uložených počítačových údajov, znemožniť prístup k takým počítačovým údajom alebo ich odstrániť z počítačového systému, do ktorého sa vstúpilo.“

služieb.[19] Procesná legitimácia povinnej osoby je definovaná buď fyzickou držbou údajov alebo štatútom poskytovateľa služieb. Teda príkaz sa bude doručovať osobe, v ktorej držbe alebo pod ktorej kontrolou sa nachádzajú také údaje alebo poskytovateľovi takých služieb (napr. prevádzkovateľovi webhostingu, cloudovej služby, účtovných služieb atď.)

Je potrebné zdôrazniť, že príkaz nemusí smerovať len priamo voči osobe, ktorá je pôvodcom počítačových údajov. Z praktického hľadiska je možné rozlíšiť medzi:

- tretími osobami, t.j. operátorom (poskytovateľom telekomunikačnej služby podľa zákona č. 351/2011 Z. z. o elektronických komunikáciách), inou osobou poskytujúcou online služby (napr. služby informačnej spoločnosti podľa zákona č. 22/2004 Zb. o elektronickom obchode) alebo vôbec neregulovanou osobou, a
- podozrivým, resp. obvineným alebo obžalovaným v zmysle TP SR.

Nakoľko procesné nároky v prípravnom konaní sú nenáročné (stačí príkaz prokurátora), prax ukázala, že využitím tohto inštitútu môže dôjsť k obchádzaniu iných informačno-technických prostriedkov (napr. odpočúvanie a záznam telekomunikačnej prevádzky, sledovanie osôb a vecí), pre ktoré sú definované vyššie kontrolné mechanizmy na ich vykonanie.[20] V súčasnosti orgány činné v trestnom konaní nemôžu bez súhlasu súdu žiadať od poskytovateľa telekomunikačnej služby (operátora) obsahové údaje. Podľa zrušeného § 116 ods. 4 TP SR, ustanovenia o zaistení prevádzkových údajov o uskutočnenej telekomunikačnej prevádzke sa primerane vzťahovali aj na obsahové údaje alebo prevádzkové údaje prenášané prostredníctvom počítačového systému. Táto skutočnosť

[19] Slovenská platná právna úprava pozná dva základné subjekty v oblasti telekomunikačnej (internetovej) prevádzky. Ide o telekomunikačného operátora, ktorý poskytuje elektronickú komunikačnú sieť alebo službu v zmysle § 5 ods. 1 zákona č. 351/2011 Z. z. o elektronických komunikáciách. Ďalším je poskytovateľ služieb informačnej spoločnosti podľa zákona č. 22/2004 Z.z. o elektronickom obchode. Z dostupnej odbornej literatúry (Rampášek) vyplýva, že sa poskytovateľom služby na účely príkazu podľa § 90 Trestného poriadku rozumie podnik podľa zákona o elektronických komunikáciách. Totiž rozdiel medzi uvedenými subjektmi je potrebný pre rozlíšenie medzi dvoma druhmi počítačových údajov, a to medzi obsahovými údajmi a prevádzkovými údajmi.

[20] Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky vydáva predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora. Viď. § 115 ods.1 zákona č.301/2005 Z. z. Trestný poriadok. In: Jednotný automatizovaný systém právnych informácií. [online]. [cit. 2015-06-12]. Dostupné z: http://jaspi.justice.gov.sk/jaspiw1/jaspiw_mini_fr0.htm

bola zmenená nedávnym rozhodnutím Ústavného súdu SR spis. zn. PL. ÚS 10/2014 zo dňa 29.4.2015, v ktorom plénum Ústavného súdu SR vyhlásilo ustanovenia § 58 ods. 5 až ods. 7 a § 63 ods. 6 zákona č. 351/2011 Z.z. o elektronických komunikáciách, ktoré doteraz prikazovali operátorom sledovať komunikáciu svojich užívateľov, ako aj § 116 zákona č. 301/2005 Z. z. Trestný poriadok a § 76a ods. 3 zákona č. 171/1993 Z. z. o Policajnom zbore, ktoré umožňovali ich sprístupňovanie, za nesúladné s ústavne garantovaným právom obyvateľov na súkromie a ochranu osobných údajov.[21]

Je možné ešte dodať, že existujú rôzne odborné názory v interpretácií ustanovení inštitútu príkazu podľa § 90 TP SR. Rampášek uvádza, že „napriek tomu, že Slovenská republika implementovala Dohovor, implementácia predovšetkým oprávnení orgánov činných v trestnom konaní pri uchovávaní a vydaní počítačových údajov bola vykonaná nesprávne, miestami až v rozpore s účelom jednotlivých ustanovení Dohovoru, pretože pripúšťa širšie, a teda neprimerané použitie implementovaných oprávnení na uchovávanie a predovšetkým vydanie počítačových údajov.“[22] Je naozaj potrebné prisvedčiť tomu, že povinnosť vydať prevádzkové údaje v zmysle § 90 TP SR nedosahuje legálny rámec nárokov už zrušeného ustanovenia § 116 TP SR.[23] Tu totiž príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke vydával písomne predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora, ktorý musí byť odôvodnený aj skutkovými okolnosťami. Navyše, tieto ustanovenia sa primerane vzťahovali aj na obsahové údaje alebo prevádzkové údaje prenášané prostredníctvom počítačového systému.

3.4 POVINNOSTI UVEDENÉ V PRÍKAZE

Príkaz musí byť v prvom rade odôvodnený skutkovými okolnosťami. Rozsah skutkových okolností síce nie je presne definovaný, avšak príkaz

[21] V súčasnosti ešte nie je k dispozícii odôvodnenie súdu. Viď. Ústavný Súd SR, Tlačová informácia č. 25/2015. [online]. [cit. 2015-06-12]. Dostupné z: http://portal.concourt.sk/plugins/servlet/get/attachment/main/ts_data/Tl_info_25_15_el_komunikacie.pdf

[22] Ibid. Rampášek, M. Uchovanie a vydanie počítačových údajov v trestnom konaní.

[23] Paradoxne, v zmysle § 90 TP SR v súčasnosti môže prokurátor vydať príkaz na vydanie prevádzkových údajov osobe, ktorá poskytuje telekomunikačné služby, ale už nemá povinnosť tieto údaje uchovávať v zmysle zákona o elektronických komunikáciách.

musí rešpektovať základné zásady trestného procesu, najmä zásadu stíhania len zo zákonných dôvodov, kedy orgány činné v trestnom konaní môžu stíhať páchateľov len spôsobom, ktorý stanoví trestný poriadok a vykonávať na to nadväzujúce úkony. Príkaz smeruje k uloženiu taxatívne určených povinností, a to aby:

a) také údaje uchovali a udržiavali v celistvosti,
b) umožnili vyhotovenie a ponechanie si kópie takých údajov,
c) znemožnili prístup k takým údajom,
d) také údaje odstránili z počítačového systému,
e) také údaje vydali na účely trestného konania.[24]

Za najzásadnejší prienik do základných práv dotknutého subjektu sa považuje posledná povinnosť, t.j. vydania počítačových údajov. Pôvodným účelom príkazu bolo v zmysle článkov 16 až 18 Dohovoru urýchlené uchovanie uložených počítačových údajov, teda zabezpečenie elektronického dôkazného prostriedku pre budúce dokazovanie. V odbornej literatúre sa objavuje názor, že toto ustanovenie slúži aj na predĺženie plynutia šesť mesačnej lehoty podľa zákona o elektronických komunikáciách, počas ktorej podnik uchováva uvedené údaje s tým, že prokurátor môže týmto príkazom zabezpečiť, aby sa tieto legálne uchovávali aj dlhšie (jedným príkazom môže prokurátor prikázať uchovanie údajov až na 90 dní).[25] Avšak táto skutočnosť bola zmenená nedávnym rozhodnutím Ústavného súdu SR.[26]

Čo sa týka časového aspektu, v príkaze podľa § 90 odseku 1 písm. a) alebo písm. c) TP SR musí byť ustanovený čas, po ktorý bude uchovanie údajov povinnou osobou vykonávané. Avšak ide už o uchovanie uložených údajov. Tento čas môže byť až 90 dní, a ak je potrebné ich opätovné uchovanie, musí byť vydaný nový príkaz. Táto špecifikácia bola doplnená až novelou č. 262/2011 Z.z. účinnou od 1. 9. 2011. Dovtedy platilo, že v akomkoľvek príkaze musí byť ustanovený presný čas, po ktorý bude

[24] Podobné povinnosti sú stanovené v článku 16 a 21 Dohovoru.

[25] Rampášek, M. Uchovanie a vydanie počítačových údajov v trestnom konaní. Bulletin slovenskej advokácie. ISSN 1335-1079. Roč. 19, č. 5 (2013), - s. 21-26.

[26] Ústavný súd SR, Tlačová informácia č. 25/2015. [online]. [cit. 2015-06-12]. Dostupné z: http://portal.concourt.sk/plugins/servlet/get/attachment/main/ts_data/Tl_info_25_15_el_komunikacie.pdf

uchovanie údajov vykonávané, čo vyvolávalo mnohé interpretačné pochybnosti.[27]

Avšak v súčasnosti je zrejmé, že pre potreby trestného konania edičná povinnosť uvedená pod písm. b) a e) predstavuje najpoužívanejší spôsob zadováženia elektronického dôkazného prostriedku v trestnom konaní bez ohľadu na povinný subjekt (ktorá má počítačové údaje v držbe resp. pod kontrolou). Túto skutočnosť demonštruje nasledujúca staršia štatistika Generálnej prokuratúry SR:[28]

	2010	**2011**	**2012**
§ 90 ods. 1 písm. a)	7	15	26
§ 90 ods. 1 písm. b)	25	57	103
§ 90 ods. 1 písm. c)	1	1	2
§ 90 ods. 1 písm. d)	0	4	7
§ 90 ods. 1 písm. e)	15	104	88
Spolu	**48**	**181**	**226**

3.5 PROCESNÉ PODMIENKY VYDANIA PRÍKAZU

Príkaz predstavuje rozhodnutie *sui generis*, voči ktorému nie je prípustný riadny opravný prostriedok. Avšak, ústavná sťažnosť za predpokladu splnenia určitých podmienok nie je vylúčená.[29] Príkaz musí byť písomný. Na rozdiel od veci, ktorú dotknutá osoba vydáva policajtovi, prokurátorovi alebo súdu, počítačové údaje je osoba, v ktorej držbe alebo pod ktorej

[27] Nález Ústavného súdu SR sp. zn. III. ÚS 68/2010 z 25. augusta 2010 [online]. [cit. 2015-06-12]. Dostupné z: http://www.pravnelisty.sk/rozhodnutia/a87-ustavny-sud-sr-o-prehliadke-advokatskej-kancelarie-a-zaisteniu-pocitacovych-udajov

[28] Novocký, J. Zaistenie majetku a vecí v trestnom konaní – aplikačné problémy, Justičná akadémia 2013. [cit. 2014-01-12]. Dostupné z: http://www.jasr.sk/files/Zaistenie_majetku_a_veci_v_trestnom_konani_aplikacne_problemy.pdf.

[29] Viď. Nález Ústavného súdu SR sp. zn. III. ÚS 68/2010 z 25. augusta 2010 [cit. 2014-01-12]. Dostupné z: http://www.pravnelisty.sk/rozhodnutia/a87-ustavny-sud-sr-o-prehliadke-advokatskej-kancelarie-a-zaisteniu-pocitacovych-udajov

kontrolou sa tieto nachádzajú povinná vydať tomu, kto vydal príkaz (predseda senátu alebo prokurátor) alebo osobe uvedenej v príkaze.[30]

Ďalej je potrebné uviesť, že použitie tohto príkazu nie je obmedzené špecifickým výpočtom trestných činov, pri ktorých je tento príkaz možné použiť (napr. ako to je pri odposluchu alebo pri inom informačno – technickom prostriedku). Ako už bolo uvedené, príkaz v prípravnom konaní nevyžaduje súhlas sudcu alebo senátu. Táto skutočnosť sa môže negatívne odraziť aj v tom, že súčasťou zaistených počítačových údajov môže byť napr. neotvorená alebo rozpísaná pošta v cloude (resp. uložená na diskovom poli servera), uložený textový rozhovor (chat), uložená streamovaná telefonická videokonferencia viacerých účastníkov atď. Je nutné poukázať na znenie Dohovoru v čl. 14 - Rozsah procesných ustanovení, ktoré sa snaží definovať hranice signatárov v prijímaní potrebných legislatívnych a iných opatrení. Dohovor nepriamo identifikuje trestné činy, voči ktorým sa rozsah procesných ustanovení uplatňuje. Totiž každá strana uplatní právomoci a postupy uvedené len na tieto trestné činy, iné trestné činy spáchané prostredníctvom počítačového systému alebo zhromažďovanie dôkazov o trestnom čine v elektronickej forme. V tomto prípade je nutné apelovať na to, aby slovenský zákonodarca v budúcnosti revidoval pôsobnosť tohto ustanovenia v zmysle Dohovoru a taktiež rozhodnutia Ústavného súdu SR ohľadom vydávania prevádzkových údajov od osôb podnikajúcich podľa ZEK.

3.6 UKONČENIE PRÍKAZU

Zákon ďalej pozná ukončenie tohto príkazu, a to pre prípad ak uchovávanie počítačových údajov vrátane prevádzkových údajov na účely trestného konania už nie je potrebné. V tomto prípade vydá predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor bez meškania príkaz na zrušenie uchovania týchto údajov. Je potrebné dodať, že ide o vágnu formuláciu, ktorá navyše bude ťažko podliehať procesnej kontrole zo strany účastníkov alebo povinných. Tu je potrebné pripomenúť zásadu oficiality, kedy orgány činné v trestnom konaní vykonávajú úkony

[30] Hasíková, J. Počítačový údaj - zdroj dokazovania. Bulletin slovenskej advokácie. 1-2/2013. Bratislava. s. 29. Obdobne Minárik, Š. Trestný poriadok, stručný komentár. Druhé, prepracované a doplnené vydanie. Iura Edition, Bratislava. 2010. s. 315.

na základe svojej úradnej povinnosti. Čiže tie sú povinné sústavne skúmať dôvodnosť vydaného príkazu a v prípade potreby ho revidovať.

3.7 POVINNOSŤ MLČANLIVOSTI

Špeciálne je upravená povinnosť mlčanlivosti. Ako už bolo spomenuté, príkaz môže smerovať voči prevádzkovateľovi počítačového systému a nie voči pôvodcovi počítačových údajov. Preto popri tomto príkaze sa mu môže uložiť aj povinnosť zachovať v tajnosti opatrenia uvedené v príkaze. Tajnosť opatrenia smeruje k snahe zabrániť zmareniu zaistenia dôkazného prostriedku. Neuposlúchnutie príkazu je sankcionované poriadkovou pokutou v zmysle § 70 ods.1 TP SR.[31]

Pre doplnenie je možné uviesť, že povinnosť mlčanlivosti smeruje vždy do budúcnosti oproti zaisťovaniu minulých (zapísaných) údajov. Je obzvlášť potrebné si dať pozor na zle formulovaný príkaz (napr. „prikazujú sa uchovávať všetky v budúcnosti získané počítačové údaje a zachovávať o tom mlčanlivosť“). Tu môže dôjsť k tomu, že sa vykoná závažnejší zásah do práv vyšetrovaného bez procesnej kontroly súdu. Totiž takýto príkaz by *de facto* nahradil odpočúvanie (napr. streamované hovory, budúca prenášaná elektronická pošta atď.)

3.8 VÝKON PRÍKAZU

V prípade ak subjekt nevyhovie dobrovoľne príkazu, orgán činný v trestnom konaní postupuje podľa § 91 TP SR (čo je spoločný postup pre vydanie veci). Podľa tohto ustanovenia, ak vec dôležitú pre trestné konanie alebo počítačové údaje na vyzvanie nevydá ten, kto ju má pri sebe, môže mu byť na príkaz predsedu senátu a v prípravnom konaní na príkaz prokurátora alebo policajta odňatá. Policajt potrebuje na vydanie takého príkazu predchádzajúci súhlas prokurátora. Bez predchádzajúceho súhlasu ho môže vydať len vtedy, ak predchádzajúci súhlas nemožno dosiahnuť

[31] „Kto napriek predchádzajúcemu napomenutiu ruší konanie alebo kto sa voči súdu, prokurátorovi, alebo policajtovi správa urážlivo, alebo kto bez dostatočného ospravedlnenia neposlúchne príkaz, alebo nevyhovie výzve alebo predvolaniu podľa tohto zákona, toho môže sudca a v prípravnom konaní prokurátor alebo policajt potrestať poriadkovou pokutou do 1 650 eur; ak ide o právnickú osobu, až do 16 590 eur. Na možnosť uloženia poriadkovej pokuty musia byť dotknuté osoby vopred upozornené.“ § 70 ods.1 zákona č. 301/2005 Zb. Trestný poriadok In: Jednotný automatizovaný systém právnych informácií [online]. [cit. 2015-06-12]. Online. Dostupné z: http://jaspi.justice.gov.sk

a vec neznesie odklad. K odňatiu veci sa podľa možnosti priberie nezúčastnená osoba. Otázkou ostáva, čo predstavujú pojmy „pri sebe“ a „podľa možnosti“ vo svetle počítačových údajov? Taktiež je dôležité sledovať ako bude táto skutočnosť vyhodnotená súdom, resp. či bude mať vplyv na následnú zákonnosť dôkazu.[32] Problémom však ostáva, ako orgán činný v trestnom konaní vykoná príkaz na odňatie počítačových údajov, ktoré sú nelokalizovateľné alebo v sústavnom pohybe (napr. cloud, ktorého dáta sa fyzický môžu nachádzať na viacerých miestach – serverových farmách). Súdna prax o aktuálnych riešeniach týchto praktických otázok zatiaľ mlčí.

V prípade ak sa počítačové údaje nachádzajú na území SR, ich zaistenie bude predchádzať dobre zvolená kriminalistická taktika - určenie typu požadovaných údajov, určenie ich pôvodcu a najmä zistenie ich aktuálneho držiteľa. V prípade ak pôjde o údaje uložené na zahraničných serveroch (najčastejší prípad využívania služieb cloud storage akými sú DropBox, GoogleDrive, OneDrive atď.), je nutné využiť existujúci zmluvný rámec medzinárodnej spolupráce v trestných veciach a poznať *best practices v* oblasti vydávania údajov jednotlivých poskytovateľov týchto informačných služieb. Buď pôjde o vykonávanie jednotlivých úkonov právnej pomoci na základe medzinárodnej zmluvy alebo o realizáciu právnej pomoci bez zmluvného základu.[33]

---

[32] Päť kritérií zákonnosti dôkazu v trestnom konaní podľa Repíka. Viď. Repík, B. Procesní důsledky porušení předpisů o dokazování v trestním řízení. , Bulletin advokacie, 1982, s. 125-126; Musil, J., Kratochvíl, V., Šámal, P. a kol. Kurs trestního práva. Trestní právo procesní, 2003, s. 408

[33] Príkladom môže byť spolupráca členských štátov EÚ, kde základom sú články 82 a 86 Zmluvy o fungovaní Európskej únie. Dňa 29. mája 2000 Rada ministrov EÚ schválila Dohovor o vzájomnej pomoci v trestných veciach, ktorého cieľom je podporovať spoluprácu medzi justičnými, policajnými a colnými orgánmi v rámci Únie doplňovaním ustanovení v existujúcich právnych nástrojoch z 20.4.1959. Taktiež významnú rolu zohráva aj budapeštiansky Dohovor o počítačovej kriminalite zo dňa 23.11.2001. V neposlednom rade ide o Dohovor o vzájomnej pomoci v trestných veciach medzi členskými štátmi EÚ, vypracovaný Radou v súlade s článkom 34 Zmluvy o EÚ. Justičná spolupráca v trestných veciach v rámci Európskej únie stojí na dvoch kľúčových princípoch: na uznávaní rozsudkov a súdnych rozhodnutí a taktiež na zbližovaní právnych predpisov členských štátov. Ide najmä o úpravu v prípade príkazu na zaistenie majetku a dôkazov v prípade zaisťovania elektronických dôkazov v pôsobnosti cudzieho prevádzkovateľa sociálnej siete. Vyjadrenie týchto princípov vo sfére dokazovania bolo zavŕšené v smernici Európskeho parlamentu a Rady č. 014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach. Viď. Smernica Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach. [online]. [cit. 2015-06-12]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014L0041&qid=1430677259904&from=EN

Je možné ešte spomenúť prípad riešený pred Ústavným súdom SR, kedy Protimonopolnému úradu SR vo veci „dawn raid“ bolo zakázané pokračovať ďalej v prehliadaní dátového nosiča vyšetrovaného subjektu Najvyšším súdom SR (bolo rozhodnuté o nezákonnom zásahu orgánu štátnej správy). Avšak tento skúmaný dátový nosič v zmysle ustanovenia § 89 TP SR Protimonopolný úrad následne vydal vtedajšiemu Úradu boja proti korupcii, ktorý až po jeho dôslednom prezretí vydal príkaz v zmysle § 90 TP SR na vydanie počítačových údajov. Takéto konanie vykazovalo znaky excesu orgánov činných v trestnom konaní. Napriek tomu Ústavný súd SR k námietke nezákonného dôkazu konštatoval, že „ v tomto kontexte neobstojí námietka sťažovateľov o tom, že orgán činný v trestnom konaní zadovážil dôkaz „ z otráveného stromu“. Protimonopolný úrad bol povinný na základe rozsudku Najvyššieho súdu sp. zn. 3 Sžz 1/2011 z 5. apríla 2011 a nepokračovať v prezeraní dátového nosiča, na druhej strane však týmto rozhodnutím nebola obmedzená jeho edičná povinnosť podľa § 89 TP SR a neboli ním limitované ani oprávnenia orgánov činných v trestnom konaní na postup podľa § 89 a § 90 TP SR.“[34] Aj keď ustanovenie je pokrokové a počíta s odňatím počítačových údajov, jeho faktická realizácia môže byť komplikovaná. Zdá sa, že pri odňatí je celá koncepcia prísne viazaná na dátový nosič – vec. Očakáva sa súdna interpretácia a stanovenie zákonných medzí tohto úkonu.

Zákon pre vykonanie procesných úkonov stanovuje náležitosti zápisnice. Zápisnica alebo potvrdenie o zaistení počítačového údaja často predstavuje ťažiskový dokument pre kontrolu legálnosti takéhoto zásahu. Zápisnica musí obsahovať dostatočne presný opis vydanej veci, odňatej veci, prevzatej veci (dátového nosiča) alebo počítačových údajov (napr. meno a špecifikáciu zaistených súborov, resp. partícií diskov), ktoré umožnia určiť ich totožnosť. Osobe, ktorá vec alebo počítačové údaje vydala alebo ktorej boli vec alebo počítačové údaje odňaté, alebo od ktorej boli vec alebo počítačové údaje prevzaté, vydá orgán, ktorý úkon vykonal, ihneď písomné potvrdenie o prevzatí veci alebo počítačových údajov alebo rovnopis zápisnice. Podstatné je ustanovenie ods.2 druhá veta § 93 TP SR, ktoré hovorí, že „osobu, ktorej počítačové údaje boli zaistené, o tom

[34] Viď. Uznesenie Ústavného súdu SR, spis. zn. III. ÚS 24/2012-53zo dňa 17.1.2012. [online]. [cit. 2015-06-12]. Dostupné z: http://www.concourt.sk/SearchRozhodnutiav01/rozhod.do?urlpage=dokument&id_spisu=422752

písomne vyrozumie orgán, ktorý počítačové údaje prevzal.“ Toto ustanovenie môže spôsobovať interpretačný problém, či ide o osobu, ktorá má v držbe tieto údaje alebo o osobu, ktorá je ich pôvodcom. Aj keď gramatickým výkladom sa dá vyvodiť záujem zákonodarcu chrániť procesné postavenie pôvodcu (zákonná záruka), súčasná prax orgánov činných v trestnom konaní ukazuje na to, že tie sú na akékoľvek informácie skúpe a tieto dotknuté osoby žiadnym spôsobom neinformujú v prípade, ak zaisťujú počítačové údaje v detencii tretích osôb.[35] Správny postup by mal byť ten, kedy orgán činný v trestnom konaní informuje pôvodcu údajov. Takáto informácia môže byť vykonaná ústne, elektronicky alebo písomne, avšak musí byť vierohodne zaznamená vo vyšetrovacom alebo súdnom spise.

4. ÚVAHA DE LEGA FERENDA

Aj keď súčasná judikatúra ESĽP nevyžaduje explicitnú zákonnú úpravu pre zaistenia počítačových údajov,[36] je v závere vhodné poukázať na niektoré pozitíva tohto inštitútu oproti všeobecnej edičnej povinnosti podľa § 89 TP SR (resp. § 78 TŘ ČR) alebo domovej prehliadke podľa § 99 TP SR (resp. § 82 TŘ CŘ).[37]

V prípade zaistenia počítačových údajov priamo z dátového nosiča – veci (napr. viaceré diskové polia, vysoko kapacitné úložiská), organ činný v trestnom konaní má zákonnú možnosť selektovať a citlivo vyberať tie

---

[35] Svedčí o tom prípad, kedy príkaz na uchovávanie počítačových údajov špeciálna prokuratúra adresovala samotnému vyšetrovateľovi policajného zboru: „ V súvislosti s vybavením podnetu prokurátor konštatoval, že je pravdou, že 18. mája 2011 protimonopolný úrad „zápisnične“ vydal inkriminovaný disk vyšetrovateľovi úradu boja proti korupcii, ale zároveň dodal, že pri postupe podľa § 89 ods. 1 Trestného poriadku nedochádza k vydaniu rozhodnutia. […] Okrem toho prokurátor konštatoval, že vzhľadom na to, že sa javilo, že na vydanom disku sa nachádzajú počítačové údaje a že tieto je potrebné uchovať, udržiavať v celosti, prípadne vyhotoviť a ponechať si orgánmi činnými v trestnom konaní kópie takých údajov, 27. mája 2011 vydal [prokurátor špeciálnej prokuratúry] v súlade s § 90 Trestného poriadku príkaz na uchovanie a vydanie počítačových údajov.“ Viď. Uznesenie Ústavného súdu SR, spis. zn. III. ÚS 24/2012-53zo dňa 17.1.2012. [online]. [cit. 2015-06-12]. Dostupné z: http://www.concourt.sk/SearchRozhodnutiav01/rozhod.do?urlpage=dokument&id_spisu=422752

[36] Vec Wieser a Bicos Beteiligungen GmbH proti Rakúsku. Rozhodnutie ESĽP zo dňa 16.10.2007, spis. zn. 74336/01 [online]. [cit. 2015-06-12]. Dostupné z: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-82711

[37] Výkladové stanovisko Najvyššieho štátneho zastupiteľstva por. č. 9/2001 Zb. tvrdí, že ako vec dôležitú pre trestné konanie je možné zaistiť aj výpočtovú techniku a záznamové médiá. Viď. §82 odst. 1 TŘ. Šámal, P. a kol.: Trestní řád. Komentář. 7. vydání. Praha : C. H. Beck, 2013, 4700 s. S. 1114.

údaje, ktoré sú pre trestné konanie naozaj dôležité. Je zrejmé, že odstavením celého počítačového systému môže dôjsť k závažným ekonomickým škodám na strane povinného alebo iných tretích osôb. Je pravda, že tento postup tu bolo možné dovodiť aj pred zakotvením tohto inštitútu. Avšak povinnosti akými sú uchovanie a udržiavanie v celistvosti, umožnenie vyhotovenia a ponechania si kópie údajov, znemožnenie prístupu k údajom alebo povinnosť odstránenia údajov z počítačového systému dávajú orgánom činným v trestnom konaní celú novú škálu nástrojov pre boj s počítačovou kriminalitou.

Ďalej to je otázka proporcionality zásahov. Ústavný súd SR v prípade prehliadky advokátskej kancelárie judikoval, že „záujem štátu na ochrane pred zločinnosťou zakladajúci legitímnosť zásahov do práva na súkromie pri realizácii niektorých inštitútov zaistenia osôb a vecí musí byť uvedený do rovnováhy so závažnosťou zásahu do tohto práva. Odkázal tak na princíp proporcionality.“ Podľa jeho názoru to znamená „zvoliť si pri realizácii zásahu čo najmiernejší prostriedok, ktorý je súčasne spôsobilý zabezpečiť dosiahnutie sledovaného cieľa. Je preto potrebné uprednostniť úkon uchovania a vydania počítačových údajov pred inštitútom vydania, resp. odňatia veci. V opačnom prípade znamená neproporcionálny postup konajúceho orgánu porušenie garancií práva na súkromie a spravodlivého procesu.“[38] Je možné zhrnúť, že pokiaľ existujú prostriedky, ktoré umožnia realizáciu citovaného cieľa a zároveň predstavujú menej radikálny zásah do chránených práv, je nevyhnutné použiť práve tieto prostriedky. Menej radikálny zásah do chránených práv je práve inštitút uchovania a vydania počítačových údajov oproti všeobecnej edičnej povinnosti podľa § 89 TP SR (resp. § 78 TŘ ČR). Umožňujú totiž voči tretím osobám uplatňovať miernejší prostriedok zásahu (vydanie konkrétnych počítačových údajov pred vydaním celistvého dátového nosiča, čo predstavuje krajné riešenie). Na druhú stranu je však nutné podotknúť, že praktická aplikácia princípu proporcionality v otázkach zaisťovania počítačových údajov je obzvlášť náročná v prípade osoby, ktorá je v postavení podozrivého (resp. obvineného alebo obžalovaného). Orgány činné v trestnom konaní v tomto prípade môžu čeliť obvyklému problému – rezistencii týchto osôb a musia postupovať pomocou efektívnejších zaisťovacích mechanizmov (domová

[38] Ibid. Nález Ústavného súdu SR sp. zn. III. ÚS 68/2010 z 25. augusta 2010

prehliadka, sledovanie osôb a vecí, atď.) v záujme naplnenia základného účelu trestného procesu.

V neposlednom rade je možné odporučiť, aby technická forma realizácie zaistenia počítačových údajov bola popísaná vo verejne dostupnom odporúčaní - smernici alebo vnútornom predpise policajného zboru. Každé zaistenie počítačových údajov by malo vychádzať z princípu zachovania proporcionálneho postupu, t.j. mal by byť zvolený taký postup orgánov činných v trestnom konaní, ktorý nepredstavuje väčší zásah do práv ako sú tie záujmy, ktoré sa týmto procesným postupom chránia. Taktiež by sa mala uplatňovať zásada nezmeniteľnosti otlačku počítačového údaja od jeho prvého zaistenia až po jeho vykonanie (resp. odovzdanie znalcovi). Práve táto skutočnosť by mala byť reflektovaná nielen v možnosti dotknutej osoby získať opis zápisnice alebo potvrdenia pri zaistení počítačového údaja s otlačkom (kópiou), ale aj v samotnej možnosti vyhotoviť si rovnocenný otlačok (kópiu) pre vlastnú potrebu toho, čo si odniesol orgán činný v trestnom konaní. Zaistené počítačové údaje sú súčasťou trestného spisu a osoba (najmä ak ide o osobu odlišnú od páchateľa) by mala mať postavenie zúčastnenej osoby, a teda právo do takéhoto spisu nazerať. V neposlednom rade je nevyhnutná transparentnosť v procese nakladania so zaistenými počítačovými údajmi a taktiež reálna možnosť procesnej kontroly nad spôsobom ich zaisťovania a nakladania s nimi.

5. ZÁVER

Zistenie skutkového stavu, o ktorom neexistujú dôvodné pochybnosti, a to v takom rozsahu, ktorý je nevyhnutný pre rozhodnutie, predstavuje vyjadrenie cieľu trestného práva procesného.[39] Voľba prostriedkov pre dosiahnutie tohto cieľu musí spĺňať základné požiadavky ústavnosti. Ak rekodifikačná komisia uvažuje o zavedení nového inštitútu zaistenia počítačových údajov s úmyslom zrýchliť a zjednodušiť procesné štádium zaisťovanie a vykonávania dôkazov, je možné poukázať na príklad slovenskej úpravy ako jeden z možných exemplárov. Aj keď niektoré otázky

[39] Zásada materiálnej pravdy. Viď. MS ČR: Komise pro nový trestní řád. Východiska a principy nového trestního řádu [online]. [cit. 2015-06-12]. Dostupné z: http://portal.justice.cz/Justice2/soubor.aspx?id=112883. s. 33.

slovenská súdna prax stále nevyriešila, definícia počítačových údajov sa zdá byť vhodná. Text zákona nemusí vždy za každú cenu dobiehať stav technológie (mnohé podstatné otázky sú aj tak vyriešené), ale spresnenie termínov a príkazov smerujúcich k počítačovým údajom, no najmä ich terminologické oddelenie od dátového nosiča, prispievajú lepšiemu pochopeniu procesu dokazovania. Práve jasná definícia procesných záruk dotknutej osoby pri zaisťovaní počítačových údajov predstavuje jednu z možných ciest pre budúci vývoj. Aj keď sa môže zdať, že záruky prvotne vyznievajú v prospech páchateľa, ich zakotvenie v procesnom poriadku nielenže stanoví limity špekulatívnej obhajoby, ale súčasne aj dodá sebaistotu orgánom činným v trestnom konaní vstupovať do situácií, ktoré sa predtým zdali byť nejasné.